ABSTRACT

A method is provided for generating a group digital signature wherein each of a group of individuals may sign a message M to create a group digital signature S, wherein M corresponds to a number representative of a message, $0 \leq M \leq n-1$, n is a composite number formed from the product of a number k of distinct random prime factors $p_1 \cdot p_2 \cdot \ldots \cdot p_k$, k is an integer greater than 2, and $S \equiv M^d \pmod{n}$. The method may include: performing a first partial digital signature subtask on a message M using a first individual private key to produce a first partial digital signature S_1; performing at least a second partial digital signature subtask on the message M using a second individual private key to produce a second partial digital signature S_2; and combining the partial digital signature results to produce a group digital signature S.